Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1517 04/26/13

~ Internet Sales Tax & GOP ~ People Are Talking! ~ Next-gen Xbox Soon!
~ Hacker Suspect Busted! ~ Twitter Credibility? ~ "Do Not Track" Bill!
~ New Xbox & Core Win 8! ~ Cops Nab Lulzsec Boss! ~ McAfee To Block Piracy

?
~ Google Makes Concession ~ Net Tax Being Blocked? ~ Social Media Rights?

-* Internet Requirement for Xbox *-
-* Military Grooms for Cyberspace War! *-
-* Facebook: Audit Finds Privacy Practices OK *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""""

We're still reeling from the tragedy in Boston and surrounding areas last week. Now is the time for healing, and remembering those who were directly affected during these events. We're beginning to learn more and more of the details - of both the suspects and the victims. In order to heal, it's important that we learn as much as possible - the why and the how, etc. I don't know if we'll learn everything - probably not.

The city is healing, and the people are beginning move forward. Boylston St. has re-opened and the people are once again mingling in an area that was terrorized. And the investigation is moving forward; they're trying to make sure that there are no stones left unturned.

It's a brief commentary, I know. Be Strong, Be Proud!

Until next time...

=~=~=~=

->In This Week's Gaming Section - Microsoft To Reveal Next-generation Xbox!
""""""""""""""""""""""""""""""" Next-gen Xbox Reportedly To Run on Core Win 8
ill Games Require Internet Connection?

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""""

Microsoft To Reveal Next-generation Xbox on May 21

Microsoft Corp will unveil its much-anticipated next-generation Xbox on May 21 following months of speculation the company is gearing up to announce a new video game console this summer.

The company sent out media invitations on Wednesday, hinting it would be announcing the successor to its seven-year old Xbox 360. A new console from the software company will come on the heels of rival Sony's announcement in February that it will launch the PlayStation4 this holiday season.

Microsoft's May event will be held at its Xbox campus in Redmond, Washington, just a month before the Electronic Entertainment Expo (E3) in Los Angeles, the gaming industry's largest annual convention, where next-generation consoles will be spotlighted.

"On May 21, we'll mark the beginning of a new generation of games, TV and entertainment," the company said on its official blog.

The Xbox 360 is the market-leading console that has an installed user base of 76 million. Gaming blogs have been afire with speculation about what features a next-generation console might offer, but Microsoft has been tight-lipped so far.

The current version of the Xbox sports voice- and gesture-command capabilities.

Next-gen Xbox Will Reportedly Run on Core Windows 8

Even if PC sales continue tanking, Windows 8 could get a significant boost in adoption later this year just from eager gamers picking up the next-generation Xbox. Paul Thurrott of WindowsITPro reports that the next-generation Xbox will release in early November and will run on the core version of Windows 8 that suggests a common apps platform or at least one that is similar to that used by Windows 8. Thurrott speculates that Microsoft could use the common app development platform as a way to open up this platform to enthusiast developers and encourage more development of native Xbox apps.

As far as pricing goes, Thurrott says that the Xbox will cost $299 up front if users sign a two-year service agreement for an Xbox LIVE Gold membership that will cost $10 per month. If users don t want to pay for a Gold membership, they can buy the standalone Xbox for $499. Thurrott also says that the next Xbox will require a connection to the Internet to use, although he cautions that this feature isn t as Draconian as many seem to believe. And finally, Thurrott says that Microsoft has for now ditched the idea of releasing an entertainment-only Xbox that would function more like a television set-top box and wouldn t have any gaming capabilities.

Next-gen Xbox To Let Publishers Decide Whether Games Require Internet Connection

The next-generation Xbox is expected to include high-end hardware and a

variety of software improvements when Microsoft announces the system next month. According to a new report from Polygon, the console will incorporate the controversial requirement that users will need an Internet connection to play some games, although the decision on whether a game will require a constant Internet will be decided by the game s publisher. Polygon warns that Microsoft s current guidelines can still change, however.

The report goes on to claim that the next-generation Xbox will include the ability to capture gameplay videos that can then be shared across different social networks, similar to the Share button on PlayStation 4's controller. Microsoft is said to be working on a DVR-like system that will allow users to record gameplay, and go back and select highlights. Users will have the option to disable or enable the function, or even set it up to automatically capture certain in-game achievements such as making a headshot or collecting a specific item.

Along with giving developers and publishers more control over copyright protection of their games, they will also have the ability to add more achievements to a game after it is launched, without having to add it as optional downloadable content.

The latest rumors suggest the next-generation Xbox will be released in early November for only $299. The system is rumored to be equipped with a 1.6GHz 8-core AMD processor, 8GB of RAM, an 800MHz graphics processor, a Blu-ray Disc drive, Gigabit Ethernet connectivity and support for core Windows 8 apps.

Microsoft will unveil the next Xbox at a press event on May 21st.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Dutch Cyberattack Suspect Arrested in Spain

Prosecutors say a Dutch citizen has been arrested in Spain in connection with what experts described as the biggest cyberattack in the history of the Internet, launched against an anti-spam watchdog group last month.

The Netherlands National Prosecution Office said a 35-year-old suspect it identified only by his initials, S.K., was arrested Thursday at his home in Barcelona. Authorities also seized computers and mobile phones.

According to a prosecution statement Friday, the man is suspected of "unprecedentedly serious attacks on the non-profit organization Spamhaus."

He was held on a European arrest warrant and is expected to be extradited to the Netherlands to face justice.

The so-called denial-of-service attack on Spamhaus fired a torrent of data

at the organization’s servers and was blamed for other disruptions online.

Australian Cops Nab Self-proclaimed LulzSec Leader

The lulz have been few and far between for hacker collective LulzSec lately since several of its members are facing prison terms, and now Australia s ABC News reports that Australian police have arrested an unnamed 24-year-old man who is purportedly the self-proclaimed leader of LulzSec. Police said that the alleged LulzSec hacker, who is known as Aush0k online, is a senior Australian IT professional who works for the local arm of an international IT company. The Australian Federal Police arrested the man for allegedly accessing a restricted computer system and for altering data with intent to cause harm. If convicted he could face a maximum of 12 years in prison.

Military Grooms New Officers for War in Cyberspace

The U.S. service academies are ramping up efforts to groom a new breed of cyberspace warriors to confront increasing threats to the nation’s military and civilian computer networks that control everything from electrical power grids to the banking system.

Students at the Army, Navy and Air Force academies are taking more courses and participating in elaborate cyberwarfare exercises as the military educates a generation of future commanders in the theory and practice of computer warfare.

The academies have been training cadets in cyber for more than a decade. But the effort has taken on new urgency amid warnings that hostile nations or organizations might be capable of crippling attacks on critical networks.

James Clapper, director of national intelligence, called cyberattack the top threat to national security when he presented the annual Worldwide Threat Assessment to Congress this month. "Threats are more diverse, interconnected, and viral than at any time in history," his report stated. "Destruction can be invisible, latent, and progressive."

China-based hackers have long been accused of cyber intrusions, and earlier this year the cybersecurity firm Mandiant released a report with new details allegedly linking a secret Chinese military unit to years of cyberattacks against U.S. companies. This year, The New York Times, The Wall Street Journal and The Washington Post all reported breaches in their computer systems and said they suspected Chinese hackers. China denies carrying out cyberattacks.

On Tuesday, hackers compromised Associated Press Twitter accounts and sent out a false tweet. AP quickly put out word that the report was false and that its accounts had been hacked. AP’s accounts were shut down until the problem was corrected.

Once viewed as an obscure and even nerdy pursuit, cyber is now seen as one of the hottest fields in warfare "a great career field in the future," said Ryan Zacher, a junior at the Air Force Academy outside

Colorado Springs, Colo., who switched from aeronautical engineering to computer science.

Last year the U.S. Naval Academy in Annapolis, Md., began requiring reshmen to take a semester on cybersecurity, and it is adding a second required cyber course for juniors next year.

The school offered a major in cyber operations for the first time this year to the freshman class, and 33 midshipmen, or about 3 percent of the freshmen, signed up for it. Another 79 are majoring in computer engineering, information technology or computer science, bringing majors with a computer emphasis to about 10 percent of the class.

"There’s a great deal of interest, much more than we could possibly, initially, entertain," said the academy’s superintendent, Vice Adm. Michael Miller.

Since 2004, the Air Force Academy has offered a degree in computer science-cyberwarfare initially called computer science-information assurance that requires cadets to take courses in cryptology, information warfare and network security in addition to standard computer science. The academy is retooling a freshman computing course so that more than half its content is about cyberspace, and is looking into adding another cyber course.

"All of these cadets know that they are going to be on the front lines defending the nation in cyber," said Martin Carlisle, a computer science professor at the Air Force Academy and director of the school’s Center for Cyberspace Research.

About 25 Air Force cadets will graduate this year with the computer science-cyberwarfare degree, and many will go on to advanced studies and work in their service’s cyber headquarters or for U.S. Cyber Command at Fort Meade, Md., the Defense Department command responsible for defensive and offensive cyberwarfare.

Almost every Army cadet at the U.S. Military Academy at West Point, N.Y., takes two technology courses related to such topics as computer security and privacy. West Point also offers other cyber courses, and a computer security group meets weekly. One of the biggest cybersecurity challenges is keeping up with the head-spinning pace of change in the field.

"You know American history is pretty much the same" every year, said Lt. Col. David Raymond, who teaches a cybersecurity course. "In this domain, it’s really tough to keep up with how this thing evolves."

In his congressional report, Clapper noted that the chance of a major attack by Russia, China or another nation with advanced cyber skills is remote outside a military conflict but that other nations or groups could launch less sophisticated cyberattacks in hopes of provoking the United States or in retaliation for U.S. actions or policies overseas. South Korea accused North Korea of mounting a cyberattack in March that shut down thousands of computers at banks and television broadcasters.

Gen. Keith Alexander, head of U.S. Cyber Command, told Congress in March the command is creating teams to carry out both offensive and defensive operations. A spokesman said the command is drawing cyber officers from the service academies, officer schools and Reserve Officer Training Corps programs.

Teams from the three academies compete in events such as last week's National Security Agency Cyber Defense Exercise, in which they try to keep simulated computer networks running as an NSA "aggressor team" attacks. Teams from the U.S. Coast Guard and Merchant Marine academies also took part, along with graduate students from the U.S. Naval Postgraduate School and Canada's Royal Military College.

Air Force won among undergraduate schools. The Royal Military College won among graduate schools.

That hands-on experience is invaluable, said 2nd Lt. Jordan Keefer, a 2012 Air Force Academy graduate now pursuing a master's degree in cyberoperations at the Air Force Institute of Technology.

"You can't just go out there and start hacking. That's against the law," he said. The competitions, he said, "gave me actual experience defending a network, attacking a network."

Counterterrorism expert Richard Clarke, noting that really high-level computer skills are rare, suggested the military might have to re-examine some of its recruiting standards to attract the most adept cyberwarriors.

"Hackers are the 1 percent, the elite and the creators," said Clarke, who served as White House cybersecurity adviser during the Clinton administration. "I wouldn't worry a whole heck of a lot (about whether they) can they run fast or lift weights."

Cyber's appeal was enough to get Keefer to put aside his dream of becoming a fighter pilot, a job with undeniable swagger. "It's a challenge, and for people who like a challenge, it's the only place to be," Keefer said.

Google Makes Concessions to EU Antitrust Body

Google is offering major concessions on how it displays search results in Europe including a better labeling of its own promoted content and displaying links to its competitors to appease concerns it might be abusing its dominant market position, the European Union's antitrust body said Thursday.

Google's search engine, which is the world's most influential gateway to online information and commerce, enjoys a near-monopoly in Europe. The EU Commission, which acts as the 27-nation bloc's antitrust authority, has since 2010 been investigating whether the company is unfairly stifling competition. It pointed out several areas of concern that Google is now trying to address through the proposed concessions.

Google has offered to more clearly label search results stemming from its own services such as YouTube, Google Maps or its shopping search function, allowing users to distinguish between natural search results and others promoted by Google. It also agreed to display some search results from its competitors and links to their services, the EU Commission said.

The Commission has often taken a harder line with U.S. tech companies than its American counterparts, the Federal Trade Commission and the Justice Department. Google, which is based in Mountain View, California, was able to settle a similar antitrust complaint on its search business with the FTC in January without making any major concessions on how it runs its

search engine.

The Commission is now proposing a market test of the concessions for a month as a test run. That would give competitors the chance to say whether they deem them sufficient.

Once the Commission accepts them revised or not they become legally binding for the company for the next five years. Google has worked closely with the Commission on the concessions' design until formally submitting them earlier this month.

"The objective of this process is to try to see if we can achieve a settled outcome in this antitrust investigation," said Commission spokesman Antoine Colombani.

The Commission said Google will "clearly separate promoted links from other web search results by clear graphical features" and "display links to three rival specialized search services close to its own services, in a place that is clearly visible to users."

Google will also give all websites the option to keep their content from being used in Google's specialized search services, "while ensuring that any opt-out does not unduly affect the ranking of those web sites in Google's general web search results," it said.

In addition, the proposed remedies will give newspaper publishers greater control over what appears in Google's news aggregator Google News. Google is also giving marketers greater ability to buy ads on rival networks.

The Commission's investigation was initially triggered by complaints from Google's rivals such as Microsoft Corp.

Google's web search service has a market share of over 90 percent in the EU, a bloc of over 500 million people that makes up the world's largest economy.

Internet Sales Tax Embraced by No-tax Republicans

You don't see this very often: a majority of Senate Republicans voting to make people who buy stuff on the Internet pay state and local sales taxes.

Anti-tax guru Grover Norquist isn't happy about it, and the conservative Heritage Foundation is questioning the senators' conservative credentials. But the issue of taxing Internet sales is getting strong support from Republicans and Democrats alike.

The Senate could vote as early as Thursday on a bill to empower states to require online retailers to collect state and local sales taxes for purchases made over the Internet. Under the bill, the sales taxes would be sent to the states where a shopper lives.

On Wednesday, the bill passed a test vote in the Senate, 74 to 23, with 27 Republicans voting in favor. Senators were trying to work out agreements Thursday on potential amendments and the timing of a final vote.

If they can't reach agreement to vote earlier, Senate Majority Leader Harry Reid, D-Nev., said, the Senate will vote Friday morning to end the

debate. The Senate is scheduled to go on vacation next week, and Reid vowed Thursday to pass the bill before senators leave town.

"This is a matter of equity and fairness," said South Dakota Gov. Dennis Daugaard, a Republican. "The same people who are selling the same products should be paying the same taxes."

Under current law, states can only require stores to collect sales taxes if the store has a physical presence in the state. As a result, many online sales are essentially tax-free, giving Internet retailers an advantage over brick-and-mortar stores.

It is part of GOP orthodoxy to oppose higher taxes, a central issue that divides Democrats and Republicans. That's why the bill faces an uncertain fate in the House, where some Republicans regard it as a tax increase.

But supporters of the bill insist it is not a tax increase. Instead, they say, the bill merely provides states with a mechanism to enforce current taxes.

"This bill has nothing to do with imposing any kind of new tax or revenue generator," said Sen. Bob Corker, R-Tenn. "What this law does is allow states that already have laws on the books to carry out the implementation of those" laws.

In many states, shoppers are required to pay unpaid sales taxes when they file their state income tax returns. In South Dakota, which has no state income tax, taxpayers are supposed to pay a use tax on out-of-state purchases. But Daugaard said the law is widely ignored.

"The difficulty is consumers don't understand the law," Daugaard said. "I think that's true in many other states as well."

The bill's main sponsor is Sen. Mike Enzi, a conservative Republican from Wyoming. He is working closely with Sen. Dick Durbin, a liberal Democrat from Illinois. Both senators say the bill is about fairness for local businesses that already collect sales taxes, and lost revenue for states.

Opponents say the bill would impose complicated regulations on retailers and doesn't have enough protections for small businesses. Businesses with less than $1 million a year in online sales would be exempt.

Many of the nation's governors Republicans and Democrats have been lobbying the federal government for years for the authority to collect sales taxes from online sales.

The issue is getting bigger for states as more people make purchases online. Last year, Internet sales in the U.S. totaled $226 billion, up nearly 16 percent from the previous year, according to Commerce Department estimates.

The National Conference of State Legislatures estimates that states lost $23 billion last year because they couldn't collect taxes on out-of-state sales.

Daugaard estimates that South Dakota loses $48 million to $58 million a year, important revenue for a state that doesn't have an income tax.

The main opposition in the Senate is coming from three states that have no sales taxes: New Hampshire, Montana and Oregon. Delaware doesn't have a

sales tax, either, but both Delaware senators have voted to advance the bill.

"We don’t like the idea of other states auditing our businesses," said Sen. Jeff Merkley, D-Ore. "They don’t like the idea of being subject to both bureaucrats and potential legal action."

Norquist, president of Americans for Tax Reform, says the bill is about "money-hungry state legislators."

"This is a dangerous road to travel, and sets precedent for further expansions of state-level tax collection authority," Norquist says in a letter to supporters. "Take action now to urge your senators to oppose an Internet sales tax scheme that lets liberal states like California and Illinois tax across their borders!"

The Heritage Foundation says that "real conservatives" oppose the bill and that it would hurt online commerce, force small businesses to jump through new bureaucratic hoops and erode state sovereignty.

But Republican Sen. Lamar Alexander, a former Tennessee governor, said the bill enhances states’ rights because it gives states the authority to enforce their tax laws.

"Tennessee wants to avoid a state income tax and treat businesses fairly in the marketplace, and it shouldn’t have to play ’Mother, May I?’ with the federal government to do so," Alexander said.

Few Senators Block Vote on Internet Sales Tax Bill

A handful of senators from states without sales taxes are blocking a bill that would tax Internet purchases.

They don’t have enough support to kill the bill, but they can delay a final vote until Friday — or even this weekend — if senators don’t reach an agreement to vote earlier.

The bill would empower states to require online retailers to collect state and local sales taxes for purchases made over the Internet. Under the bill, the sales taxes would be sent to the states where a shopper lives.

Sen. Ron Wyden, D-Ore., is leading the fight against the bill. Oregon, Montana, New Hampshire and Delaware have no sales taxes, though the two senators from Delaware support the bill.

"It’s coercive. It requires a number of states to collect the taxes of other states thousands of miles away against their will," Wyden said in an interview. "It’s discrimination because this forces some people online to carry out responsibilities that brick and mortar retailers do not have to do."

Wyden said the bill also gives an advantage to foreign retailers. Supporters say the bill treats foreign retailers the same as domestic ones, but opponents question the ability of states to enforce state tax laws on companies based in other countries.

The bill has already survived two procedural votes this week, getting 74 votes in favor each time. If senators don't reach an agreement to vote earlier, Senate Majority Leader Harry Reid, D-Nev., threatened to hold a vote shortly after midnight Friday morning to end the debate.

The Senate is scheduled to go on vacation next week, and Reid vowed to pass the bill before senators leave town.

"One way or another, we will finish work on this measure before we leave," Reid said.

Wyden said he doesn't want to inconvenience senators eager to go home. But, he added, "I don't want to have our constituents rolled over in the process."

Under current law, states can only require stores to collect sales taxes if the store has a physical presence in the state. As a result, many online sales are essentially tax-free, giving Internet retailers an advantage over brick-and-mortar stores.

Supporters say the bill is about fairness for local businesses that already collect sales taxes, and lost revenue for states. Opponents say the bill would impose complicated regulations on retailers and doesn't have enough protections for small businesses. Businesses with less than $1 million a year in online sales would be exempt.

Many of the nation's governors Republicans and Democrats have been lobbying the federal government for years for the authority to collect sales taxes from online sales.

The issue is getting bigger for states as more people make purchases online. Last year, Internet sales in the U.S. totaled $226 billion, up nearly 16 percent from the previous year, according to Commerce Department estimates.

The National Conference of State Legislatures estimates that states lost $23 billion last year because they couldn't collect taxes on out-of-state sales.

The bill pits brick-and-mortar stores like Wal-Mart against online services such as eBay. The National Retail federation supports it. And Amazon.com, which initially fought efforts in some states to make it collect sales taxes, supports it, too.

The bill also gets support from many Republicans who have pledged not to increase taxes. The bill's main sponsor is Sen. Mike Enzi, a conservative Republican from Wyoming. He is working closely with Sen. Dick Durbin, a liberal Democrat from Illinois.

Enzi and Durbin say the bill doesn't raise taxes. Instead, they say, it gives states a mechanism to enforce current taxes.

In many states, shoppers are required to pay unpaid sales taxes when they file state tax returns. But governors complain that few people comply.

Sen. Chris Coons, D-Del., said he supports the bill in part because tax-free Internet sales are eating into sales by Delaware retailers.

"In our region, we've long benefited from significant commercial sales from residents of Maryland, of New Jersey, Pennsylvania and elsewhere,

who come to Delaware to shop because we're a tax-free state," Coons said. "Over time, the benefit of that has eroded as folks discovered that they could buy the same things online without paying sales tax from home."

He noted that the bill would not require anyone from Delaware to pay sales taxes.

Senate Chairman Calls for 'Do Not Track' Bill

Warning consumers that industry has failed to protect their privacy online, a top Senate Democrat said Wednesday that he will press legislation this year that would create a universal "Do Not Track" option for consumers and penalize companies that fail to honor it.

"The American people are smart," said Sen. Jay Rockefeller, D-W.Va., chairman of the Senate Commerce Committee. "They are going to figure this out. And as they figure this out, they better like what they see if the Internet is going to prosper."

Rockefeller's proposal could face an uphill battle in a divided Senate already consumed with immigration and the budget. But his comments put renewed pressure on an industry struggling desperately to escape regulation.

The online privacy debate has mostly stumped Congress and prompted a tempered reaction from the Obama administration, mindful of consumers' concerns but reluctant to crush a growing industry in a difficult economy. Last year, the White House unveiled a "Consumer Privacy Bill of Rights" calling on industry to give consumers more control over their personal information and suggesting Congress pass legislation to enforce it.

But while everyone agrees that people should be given a choice to opt out of data collection and online tracking, advertising businesses and privacy groups remain at odds over how to implement it. Much of the debate focuses on whether consumers should have to click an opt-out button, or if their browser should automatically do it for them.

Rockefeller said Wednesday that voluntary efforts by industry have fallen short because some online advertisers ignore consumer requests not to be tracked. His bill would subject businesses to penalties by the Federal Trade Commission if they do.

"I do not believe that companies with business models based on the collection and monetization of personal information will voluntarily stop those practices if it negatively impacts their profit margins," Rockefeller said.

Industry is pushing back. The Digital Advertising Alliance points to its Web-based icon program that links consumers to an opt-out site of participating advertisers. They say some 20 million people have visited their site and only 1 million of those consumers chose to opt out of all ad tracking. Testifying at the hearing, Mastria said he thinks the industry has "delivered basically in principle" what Rockefeller proposes through legislation.

"Consumers are very pragmatic people," Lou Mastria, managing director of the Digital Advertising Alliance, said in an interview this week. "They

want free content. They understand there’s a value exchange. And they’re OK with it."

The Do Not Track proposal is part of a broader debate about online privacy that includes what sensitive data might be collected from a person’s mobile device. Because a smartphone can divulge a person’s location, the FTC warned in a recent report that detailed profiles of a person’s movements can be collected over time and in surprising ways, revealing a person’s habits and patterns and making them vulnerable to stalking or identity theft.

Some researchers also say they suspect retailers are engaging in "price discrimination" the practice of setting a price based on personal data, such as the average home price in their area or a person’s proximity to a competitor.

Another concern is that companies might determine a person’s eligibility for certain products and services based on information collected online, potentially violating credit reporting and fair lending laws.

"I think there should be obligations for companies to tell you what information they have about you" and give you the opportunity to correct it, said Justin Brookman of the Center for Democracy and Technology.

Adam Thierer, a senior research fellow at George Mason University’s Mercatus Center, told the Senate panel that he thinks many of the privacy concerns cited with data collection are worst-case scenarios that probably won’t happen. In the end, he said, data collection is merely "creepy" and might not warrant legislation.

"I think a lot of my neighbors are creepy, but I don’t think they’re harmful," Thierer said.

Missouri Court Rules Against $440,000 Cyberheist Victim

A Missouri court last week handed a legal defeat to a local escrow firm that sued its financial institution to recover $440,000 stolen in a 2009 cyberheist. The court ruled that the company assumed greater responsibility for the incident because it declined to use a basic security precaution recommended by the bank: requiring two employees to sign off on all transfers.

courthouseSpringfield, Mo. based Choice Escrow and Land Title LLC sued Tupelo, Miss. based BancorpSouth Inc., after hackers who had stolen the firm s online banking ID and password used the information to make a single unauthorized wire transfer of $440,000 to a corporate bank account in Cyprus.

Choice Escrow alleged that BancorpSouth s security procedures were not commercially reasonable. Choice pointed out that the bank s most secure option for Internet-based authentication relied principally on so-called dual controls, or requiring business customers to have one user ID and password to approve a wire transfer and another user ID and password to release the same wire transfer.

Choice Escrow s lawyers argued that because BancorpSouth allowed wire or funds transfers using two options which were both password-based, its

commercial online banking security procedures fell short of 2005 guidance from the Federal Financial Institutions Examination Council (FFIEC), which warned that single-factor authentication as the only control mechanism is inadequate for high-risk transactions involving the movement of funds to other parties.

But in a decision handed down on March 18, 2013, a judge with the U.S. District Court for the Western District of Missouri focused on the fact that Choice Escrow was offered and explicitly declined in writing the use of dual controls, thereby allowing the thieves to move money directly out their account using nothing more than a stolen username and password. The court noted that Choice also declined to set a limit on the amount or number of wire transfers allowed each day (another precaution urged by the bank), and that the transfer amount initiated by the thieves was not unusual for Choice, a company that routinely moved large sums of money.

Like most U.S. states, both Missouri and Mississippi have adopted the Uniform Commercial Code (UCC), which holds that a payment order received by the [bank] is effective as the order of the customer, whether or not authorized, if the security procedure is a commercially reasonable method of providing security against unauthorized payment orders, and the bank proves that it accepted the payment order in good faith and in compliance with the security procedure and any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer.

The Choice Escrow judgment may be among the first to focus on a particular aspect of the UCC (Article 4a), which states that if the bank offers to the customer a security procedure which the customer declines, the bank can argue that its procedures were commercially reasonable, said Dan Mitchell, an attorney in Portland, Me.

Really, it looks like that s what this whole case was about for the court, which didn t examine whether the bank s security procedures were commercially reasonable, said Mitchell, who recently represented Patco, a Maine construction firm that successfully sued its bank for poor security following a $588,000 cyberheist that also took place in 2009. The court s whole analysis was about the fact that the bank offered dual controls which the customer declined.

Charisse Castagnoli, a bank fraud expert and independent security consultant, said the fraud incident happened before banking regulators issued the current online banking security guidelines, which call on banks to take additional steps to protect customers from account takeovers including educating customers about the sophistication of today s threats.

The bank s security may not have been sufficient by today s standards, but the key here was that the bank offered a security measure that was refused, Castagnoli said. If the bank doesn t ever make the recommendation to use additional controls, then shame on them. But in this case, it seems like the bank was trying to steer their customer to use those controls. Considering this was back in 2009, it looks like the bank was at least doing a pretty good job informing their customers about the need for dual controls.

Choice Escrow declined to comment, or say whether it planned to appeal. But according to Castagnoli, summary judgments can be difficult to appeal. It s pretty expensive, and the standard of review for the court is fairly high.

There is no doubt that requiring two employees to sign off on all transactions minimizes the potential for fraud (particularly employee/insider fraud). But dual controls alone are hardly sufficient. The very first cyberheist case that I wrote about back in the summer of 2009 dealt with the electronic theft of $415,000 from Bullitt County, Kentucky. Bullitt had set things up so that all payments had to be initiated by the county treasurer and approved by the county judge.

In that attack, the crooks had compromised the treasurer s computer, which allowed them to change the email addresses that were to receive notifications about new transactions. They were able to do this because the treasurer was the designated administrator of the county s account settings at the bank. They then changed the judge s password in the bank s system, and approved the fraudulent transfers using a computer outside of the state of Kentucky.

The best way to avoid a cyberheist is to not have your computer systems infected in the first place. The trouble is, it s becoming increasingly difficult to tell when a system is or is not infected. That s why I advocate the use of a Live CD approach for online banking: That way, even if the underlying hard drive is infected with a remote-access, password stealing Trojan like ZeuS or Citadel, your online banking session is protected. This is just one of the tips from a much longer list of precautions that small- to mid-sized businesses should consider adopting when banking online.

McAfee Working on Software That Finds and Blocks All Pirated Content

McAfee may be about to become the best friend of copyright holders all over the world. TorrentFreak reports that McAfee has patented a new technology that aims to prevent the public from accessing pirated movies and music online. The content-blocking technology could be integrated with McAfee s SiteAdvisor toolbar and would essentially create a blacklist that compiles reported pirated content from across the web and offer users alternative suggestions for how to legally buy the content they re looking for. In its patent filing, McAfee writes that by informing a user of illegal sources and possible alternatives, a user can obtain the desired electronic distribution without violating an author s intellectual property rights.

Facebook: Audit Finds Privacy Practices Sufficient

Facebook says that an independent audit found its privacy practices sufficient during a six-month assessment period that followed a settlement with federal regulators.

Facebook Inc. said it submitted the findings to the Federal Trade Commission on Monday evening. The audit was a required part of the social networking company’s settlement with the FTC last summer. The settlement resolved charges that Facebook exposed details about its users’ lives without getting the required legal consent.

Facebook provided a copy of its letter to the FTC, along with a redacted copy of the auditor’s letter, to The Associated Press on Wednesday. The

redacted portion contains trade secret information and does not alter the auditor’s findings, the company said. The audit, which found that Facebook’s privacy program met or exceeded requirements under the FTC’s order, covered written policies as well as samples of its data.

"We’re encouraged by this confirmation that the controls set out in our privacy program are working as intended," said Erin Egan, Facebook’s chief privacy officer for policy," in an emailed statement. "This assessment has also helped us identify areas to work on as Facebook continues to evolve as a company, and improve upon the privacy protections we already have in place. We will keep working to meet the changing and evolving needs of our users and to put user privacy and security at the center of everything we do."

Facebook did not disclose the full, 79-page report or specific details on shortcomings in its privacy practices that were revealed by the audit. Spokeswoman Jodi Seth said Facebook declined to disclose such details "based on contractual obligations and the possibility of security and competitive vulnerabilities."

The company has asked the FTC to keep the redacted information private, saying it would put it and its auditor at a competitive disadvantage and because it could reveal possible limitations of its privacy program.

The name of the accounting firm is also redacted but that information will be released when the FTC responds to the audit.

A representative for the FTC did not immediately return a message for comment on Thursday morning.

Facebook has made several high-profile mistakes over user privacy, especially in its early years. Much of the FTC’s complaint against the company centered on a series of changes that Facebook made to its privacy controls in late 2009. The revisions automatically shared information and pictures about Facebook users, even if they previously programmed their privacy settings to shield that content. Among other things, people’s profile pictures, lists of online friends and political views were suddenly available for the world to see, the FTC alleged.

The complaint also charged that Facebook shared users’ personal information with third-party advertisers from September 2008 through May 2010 despite several public assurances from company officials that it wasn’t passing the data along for marketing purposes. Facebook said this only happened in limited instances.

Facebook did not admit any wrongdoing as part of the settlement, but it agreed to submit to audits of its privacy practices for 20 years. This was the first of those audits. Google Inc. earlier agreed to a similar settlement, but was fined $22.5 million last August to resolve allegations that it did not comply with it.

Workers Demand Social Media Rights

Employees no longer see using Facebook in the office as luxury or a business tool, but as a right, new research shows.

A quarter of employees say they would not work for a company that banned

social media at work. In total, nearly one-third of employees are spending an hour or more a day on Facebook, Twitter and other social media sites during work hours, a study by virtual office space franchise Intelligent Office found.

The study shows that those social media needs are part of an overall trend of employees desiring more choice in the technology they use. One-third of those surveyed would prefer to work for a company that allows them to use their own technology.

"Technology has made it possible to change the way we work, and now we simply see workers embracing the freedom to do so," Tom Camplese, Intelligent Office s chief operating officer, told BusinessNewsDaily.

Helping to drive the desire for more technology choices is the increasing wish among employees to work from locations outside of the office.

"We are continuing to find that in order to increase mobility without lost productivity, a new breed of worker is conducting business on the go, and wants to be able to work more independently," Camplese said."Many would argue that productivity has seen a significant boost as technology has fostered the ability to conduct business on the go, anywhere, any time."

Camplese believes this is all part of a culture shift taking place in which today’s workers are personalizing and customizing their work in many ways, including work style, location and technology.

"We have ultimately uncovered a dramatic shift in how people work today and how they want to work," he said. "We see this trend of employees wanting more choice and flexibility continuing into the future."

The study was based on surveys of more than 1,000 employees in the United States and Canada.

Truth and Consequences - A Dilemma for Twitter and Its Users

Does Twitter have a credibility problem?

For many, a single fake tweet from the Associated Press account that briefly roiled financial markets on Tuesday, driving the Dow Jones industrial average down about 145 points, vividly reaffirmed the fearsome, near-instantaneous power of the 140-character message.

But the security lapse also revived doubts about Twitter’s place in the media landscape - and its ultimate value - at a moment when its status as one of today’s essential information networks had seemed all but cemented.

Just a week after social media networks took criticism for helping circulate misinformation about the alleged perpetrators of the Boston Marathon bombing, Twitter’s security shortcomings fell under a harsh spotlight Tuesday after a hacker group commandeered the AP Twitter account and falsely reported that explosions in the White House had injured President Barack Obama.

The AP was only the latest hacking victim in recent days after Twitter accounts belonging to National Public Radio, CBS 60 Minutes and others were breached. Last year, Reuters News was the victim of hackers who

briefly took over one of its Twitter accounts and posted false tweets.

The latest hack was by far the most significant: the single AP tweet stunned investors and effectively wiped out $136.5 billion of the S&P 500 index’s value in a matter of minutes.

Although the news agency later disclosed that one of its employees may have inadvertently given away company passwords as the result of a "phishing" attack by the hackers, security experts quickly faulted Twitter for its longstanding failure to implement two-factor authentication, a double-layered password feature used by the likes of Google Inc and Microsoft Inc that might have prevented the spate of high-profile Twitter hijackings.

"It’s one of those cases that we are seeing too often. It’s getting unnerving," said Robert Quigley, a journalism lecturer specializing in social media at the University of Texas. "What media organizations need to do is pressure Twitter to have a more secure website."

The company has also repeatedly declined to discuss its product roadmap, although it has signaled that it will soon unveil two-factor authentication, including a public job posting in February that suggested it was hiring to tackle the problem.

Mark Risher, the founder of a security consultancy that counts social media companies Pinterest and Tumblr among its clients, said introducing more measures like two-factor authentication would make Twitter more cumbersome to use and potentially slow its user growth - a critical concern for a company that relies on advertising revenues. But he warned that a prolonged rash of high-profile hacks, and an eroding sense of user trust, would hurt Twitter more.

"There’s always a tradeoff between convenience and safety," Risher said. "But a security issue damages Twitter’s brand."

For Twitter, the hacking has raised questions about its credibility just as it is beginning to assume a central role in a fast-changing media landscape, with the volume of tweets rising to more than 400 million a day. Earlier this month, the Securities and Exchange Commission ruled that U.S. companies may report material information such as quarterly results on Twitter, as long as investors are alerted in advance. Days later, Bloomberg L.P. said it would funnel Twitter directly into its terminals used by thousands of traders on Wall Street.

At the same time, the world’s leading news organizations and Twitter, which has 200 million users around the world, have become increasingly intertwined in a symbiotic, if sometimes troublesome, relationship.

Dan Gillmor, a journalism professor at Arizona State University, said the hacks have especially hurt news outlets because their Twitter accounts are often the primary way that their news reaches consumers who may not subscribe to a newspaper or have access to a newswire.

Twitter has touted itself as a critical newswire of sorts, such as during the 2011 tsunami in Japan, when it helped emergency responders locate survivors, or when it became a vital lifeline for some New Yorkers as television sets fell dark during Hurricane Sandy last year.

But last week, in the wake of the Boston bombings, some of those who previously viewed Twitter as an indispensable news source began turning

against the service upon discovering that the wisdom of crowds is, in fact, an adage not often applicable on the Internet.

Steve Brunetto, a senior executive at Edgewave, a network security company, said Tuesday's hacking undermined Twitter at a sensitive time.

"On the heels of the Boston Marathon bombing, everyone's trying to figure out, 'Okay, where does Twitter fit into that news cycle? Where does Twitter fit into disseminating information?'" Brunetto said. "They've got an opportunity to legitimize themselves as a real player in that information life cycle but they get knocked down a peg every time somebody says, 'Oh, you can't believe what you read on Twitter.'"

Jeff Jarvis, a prominent Internet pundit and a journalism professor at City University of New York, said that the confusion caused by social media in recent weeks was not an indictment of social media but rather a reminder that the onus falls on professional reporters to verify information.

"No, the Internet's not broken," Jarvis said.

The rise of social media means that "you now hear more bar-room debates and speculation than before," he added. "But that doesn't mean you should believe it more than you ever did."

Tom Schrader, managing director for U.S. equity trading at Stifel Nicolaus Capital Markets in Baltimore, said there were a lot of clues in the false AP tweet that should have kept traders from reacting, in particular the wording of the message.

"We saw it, we saw the initial reaction. Initially our reaction was, pull your bids (until we) see whether this is legit or not. We found no legitimacy to it and went back into the market as normal," he said.

Oli Freeling-Wilkinson is chief executive officer of Knowsis, a London company that picks out and amalgamates financially relevant tweets and other social media content for traders. "We do have spam controls in place, but it's an ongoing war," he said. "It's much more difficult to work out what's going on when people are hacking into official accounts, especially in the heat of the moment."

While Twitter has occasionally signaled that it believes it could become more than a passive distribution network - a shift marked by last year's purchase of Summify, a small startup that specialized in surfacing relevant news - it has also taken pains to distance itself from the content of tweets and maintain strict neutrality from a legal perspective.

Twitter Chief Executive Dick Costolo told an Online News Association gathering last autumn that Twitter's primary responsibility was to create a platform, rather than to play an editorial role in determining which tweets people should see.

"A company trying to build media is creating or curating content, and that's not the kind of company we're creating," Costolo said.

Gillmor, from Arizona State, said Twitter did not need to guarantee the quality or veracity of its content in order to grow into a media juggernaut.

"It’s not whether Twitter is credible or not, it’s what people do with it," he said. "Every news organization feels it has no alternative but to use Twitter. But everyone at the traditional news organizations has to be thinking really hard about what that means, from whether the security is sufficient on these third-party platforms to what it means to be turning part of your stuff over to new kinds of publishers."

=~=~=~=